International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Novel Security Framework for Wireless Sensor Networks

Abhishek Pandey, Lokendra Kumar Tiwari

Abstract: ***Today we can't think communication systems without support of advancements made in computer technologies whereby it is a major achievement to realize the convergence of the technologies providing highly pervasive system. The communication systems evolved essentially from wired communications and grew to the current wireless communications. Wireless sensor networks do not need large deployment infrastructure. Here each individual sensor node acts as a part of the overall infrastructure. All nodes are connected in multi-hop mesh topology. In this flexible mesh architecture, we easily add new nodes and scale up to achieve control and monitoring over larger region. The sensor network protocols and algorithms possess self-organizing capabilities. Wireless sensor network communication systems mostly being deployed in open fields are physically accessible to adversaries and are more vulnerable due to being remotely managed, densely deployed, low power (battery life time), low communication bandwidth, low processing capability, and use of only the broadcasting mechanism to communicate with other nodes[1].***

Keywords:- WSN, Security, PKI, Sybil Attack.

I. INTRODUCTION:

The traditional security mechanisms are authentication, symmetric key encryption & decryption and public key infrastructure (PKI) having built in cryptography. The major challenge is to deploy the techniques of above mechanisms or their modified incarnations in a sensor network with due regard to the WSN's being is characterized with constrained memory, power (sensor life) and processing capability. On the top of all this, the wireless sensors need very secure communication in wake of they being in open field and being based simply on broadcasting technology [1].

A. Layered Based Security Approach

Wireless sensor network broadly categorized in four layer, layer wise attacks and respected mitigation technique is given in the following table.

WSN Layer	Types of Attacks	Remedial Existing Protocols/ Techniques
Physical Layer	Denial of service attack Jamming	Multi protocol routing technique, spread spectrum technique.
	Denial of service attack Tampering	Aggregation, effective key management technique
		Anti Jamming Techniques
Data Link Layer	Denial of service attack (Collision)	Error correction
	Denial of service attack (Exhaustions)	By using threshold for rate limitation
		Link Layer Security Protocols (TinySec, PEGASIS, LEACH)
Network Layer	Denial of service attack	Authentication
	Wormholes	
	Sinkholes	
	Sybil attacks	
	Hello Flood	Routing protocols (ID based, Data Centric). PEGASIS, LEACH
Transport Layer	Denial of service attack (Flooding)	Client puzzles,
Application Layer	Malicious Node	Aggregation Scheme
	Clone attack	Unique pair-wise keys distribution

B. Routing Attacks

The security breaches occur primarily in the form of interruption (breakdown of communication links), interception (unauthorized access of WSN), modification (change of data by unauthorized access) and Fabrication (addition of false data by unauthorized accesses). On the lines of analogous attacks in data communication networks different types of routing attacks are categorized as below [2,9].

Manuscript published on November 30, 2019.
* Correspondence Author
Abhishek Pandey, Assistant Professor at IIIT-Lucknow,
Lokendra Kumar Tiwari, Assistant Professor at Ewing Christian College, University of Allahabad

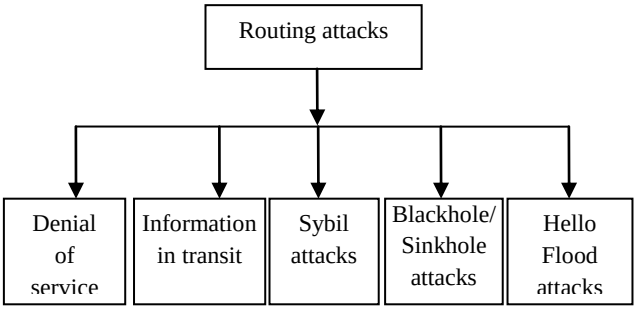

Figure 1.2

Denial of Service Attack

This type of attack results in making unavailable the resource to their intended user. As an example say node 'A' sends request to node 'B' for communication and node 'B' sends acknowledge to node 'A' but by making some modification in the communication program the adversary focus 'A' to keep on sending request to 'B' continuously. As a result 'B' is busy to send acknowledge to node 'A' and is not able to communicate with any other nodes and thus becomes unavailable to all of the nodes except 'A'.

Denial of service attack may also occur at physical layer by jamming and/or tampering of the packet. In link layer it is done by producing collision of data, exhaustion of resources and unfairness in use of networking resources. In network layer, it may occur by way of neglecting and the greediness of packets resulting into path failure. In transport layer, DOS attack occurs due to flooding and de-synchronization.Most of denial of service attacks may be prevented by powerful authentication and identification mechanisms.

Attack of Information in Transit

In case of WSN, usually each node reports changes to a cluster head or base station only for data above some threshold. Information in transit may be altered, spoofed, replayed again or vanished. In this type of attack, the attacker has high processing power and large communication range. This type of attack may be prevented by data aggregation and authentication techniques.

Sybil Attack

In this attack the attacker gets illegally multiple identities on one node (i.e. reputation based system). The vulnerability in a reputation based system depends on the cost of generation of multiple identities. By this, the attacker mostly affects the routing mechanism. When any node wants to communicate to the base station or sink, then it's most probable to transfer that data with the help of that attacker node. At that time attacker easily snoops data or alters the data. To prevent this attack by providing authentication we can use different key distribution and validation techniques.

Blackhole/ Sinkhole Attack

In a sinkhole/blackhole attack, the attacker aims at attracting the traffic in a particular area. For this, the attacker places himself in a network with high capacity resources (high processing power and high band width) by which it always creates shortest path. As a result, all data passes through attacker node, due to the high capacity resources, the attacker node makes itself stationed in a shortest path so all the nodes in the networks send data via attacker node so that the attacker node whereby may snoop or modify those data very easily.

'Hello Flood' Attack.

This is one of the simplest attacks in wireless sensor networks since some routing protocols require to broadcast "HELLO message" to intimate their presence to their neighbors. In this type of attack, attacker broadcasts HELLO packet with high transmission power (like laptop) to sender or receiver. The nodes receiving the messages assume that the sender node is nearest to them and send packet by this node. By this attack, congestion occurs in the network. This is a specific type of DOS attack. Blocking, node authentication techniques are used to prevent 'Hello Flood' attacks.

C. Secure key management technique

The key management technique is the best solution for achieving the security goals of confidentiality, integrity and authentication. Wireless sensor networks being adhoc in nature, are characterized with many limitations. To create a good secure key management is itself a big challenging task due to the constraints of sensor nodes in terms of hardware cost, memory space, energy provisioning and computational power. Traditional key management techniques using public key infrastructure cryptographic technique like AES RSA, Elliptic Curve cryptography and the third party authentication like Kerberos are not suitable in WSN. So we may devise some significant modifications of existing key management technology that should make wireless sensor networks secure and are practically feasible.

D. Malicious node detection technique

The mechanism for finding out the malicious node is called Intrusion detection system. Intrusion detection is a monitoring system i.e. a software/ hardware by which we can detect unwanted services in the system or network activity and identify suspicious patterns that may indicate a network or system under attack from some adversary.

An intrusion detection system is classified broadly in two categories- i) anomaly based intrusion detection (AID) and ii) misuse intrusion detection system (MIDS) based on the signature of the intruder.

Eiji Nii [3] introduced a suspicious message detection technique by using signal strength. Here the monitor node contains two values in which first is expected signal strength of the received signal as per the already maintained message transmission system and distance between node, whereas the second value is the actual signal strength of the signal. If the difference between them is more than a threshold, message is treated as suspicious.

For this work the authors took many assumptions like all nodes in a wireless sensor network have same hardware and software, WSN being static in nature, every time all nodes should have same transmission power, antenna height etc. However in real life, these assumptions do not hold good for a wireless sensor network. Anomaly based intrusion detection system(IDS) by implementing patterns. For this all hosts are provided a baseline for normal communication. Each active IDS compares all coming traffic with the baseline to detect any attack like firewall which detects all outgoing and incoming data traffic passing through this IDS system[4]. Major drawback of this technique is that to secure entire network we need IDS system at all nodes. But sensor network have limited memory and processing capability so it is a big limitation and therefore their technique did not prove very useful. AbduvaliyevAbror[5] proposed energy efficient hybrid intrusion detection system for wireless sensor networks. Here authors use both anomaly and misuse based detection. Here the author uses cluster based protocol. IDS agent is placed only on cluster head. This helps to achieve energy efficiency and compatibility to the requirement of low processing power. This IDS system broadly works in three steps. First is anomaly detection model which detects abnormal behaviors of the nodes with the help of pre-defined rules. Second is Misuse detection model. For this the author uses machine learning algorithm SLIPPER; a confidence rate boosting algorithm and generates a training data set. Third and last is Decision making model which makes final decision whether any intrusion has occurred on any node or not. It processes the result of anomaly detection as well as of misuse detection model. The authors claimed that it is an energy efficient technique of IDS because this IDS is placed only on the cluster head. The major drawback of this technique is that machine learning algorithm uses large data set so cluster head gets dead very fast. Time to time cluster head is changed so all nodes will have to store this training data set and update it at a regular interval.

II. PROPOSED SECURITY TECHNIQUES

In order to establish the WSN security merely one mechanism does not suffice. So the functioning of our three tier architecture ensures an independent working of individual layers. But to obtain total security we need to use all three layers at a time. For this, our framework comprising security at three levels is created as described below.

A. Our Key Management Technique

Sensors are used to send very short data like informations about temperature, fire etc. They are deployed densely in the field and therefore use of encryption/decryption and authentication techniques at the level of each nodes is not useful. Therefore, any improved mechanism is required for security of the sensor network. Through the current research work, we are hereby proposing a two tier based security technique for key management, which basically involves security from i) node to cluster head and ii) cluster head to the base station[8]. Here data aggregation technique is used between nodes to cluster head communication. Authentication and encryption/decryption are used only for communication between any cluster head to its base station. Details are depicted as follows in figure 2.1.

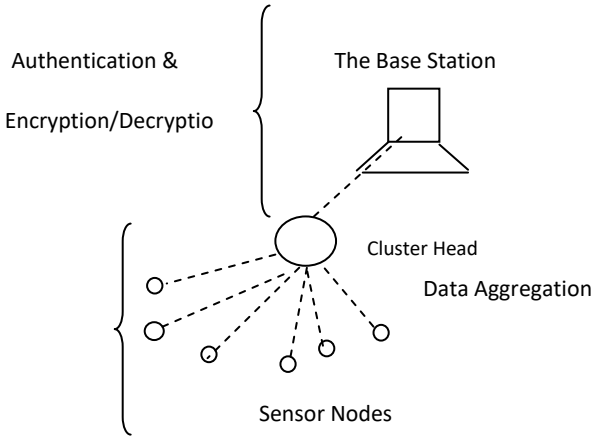

Figure 2.1 Two tier based security technique

- *Security between Nodes to their Cluster Head:* To secure the communication between a set of nodes and their cluster head, we use data aggregation technique [6]. In this technique, first we assume that all the sensor nodes are densely deployed in open field wherefrom the base station has to collect data in a unified way of a particular range. This means more than one node as such may send information which will be sensed by it since initially all nodes have equal priority. However this has the problem that even a malicious node will have same chance to send its data as a genuine node. We get rid of this situation based on data aggregation by a cluster head having enough energy in a way so that the malicious node is progressively discarded in its own cluster for this. For this we developed a priority based aggregation. The cluster head uses an aggregation function, by which cluster head detects the malicious node. Initially all nodes have equal priority which is assigned as one. After each communication cluster head updates the priority of each node according to its data. If priority goes lower than a threshold then cluster head blocks such a malicious node. Details are given as below.

Algorithm for data aggregation:

A cluster head has a data set where it stores sensor ID with its Priority

Step 1: Start aggregation function

Step 2: for i=0; to total_node

Step 3: if node(i).priority<1

Step 4: go to step 2

Step 5: temp_data=node(i).data

Step 4: aggregator= aggregator +(temp_data*node(i).priority)

Step 5: count=count+priorty

Step 6: end of loop (step 2)

Step 7: total_aggregator=aggregator/count

Step 8: for i=0 to total_node

Step 9: temp = total_aggregator~ node(i).data

Step 10: if temp<=5

Step11: node(i).priority=node(i).priority+0.5 else

Step 12: node(i).priority=node(i).priority-1

Step 13: end of loop (step 7)

- *Security between a Cluster Head to the Base Station:* For secure communication in a wireless sensor network, public key cryptosystem is not suitable due to its high computational cost. In the presently proposed research work, we therefore use symmetric key cryptosystem.

In symmetric key cryptosystem, the key (private key) distribution is a major problem. To resolve this problem, we use pseudo random number technique for authentication and encryption/decryption. To secure communication between cluster head and base station we use authentication and encryption/decryption technique. In a whole WSN network the number of cluster heads are limited whereas the base station is highly powerful. So our application program is easily implemented and its cost is also very low in comparison to other developed techniques proposed by different authors so far.

In our proposed technique, first of all we provide an unique 8 digits sensor ID and store an application program in every sensor node before their deployment in the field. For every cluster head we generate a Pseudo Random Number (PRN) and Relative Prime Number (RPN). For every sensor node elected as a cluster head, the range of PRN is different. With the help of this PRN and RPN, we generate authentication code and use a symmetric key encryption/decryption technique. Base station maintains database which stores unique Cluster head ID, Pseudo random numbers and Authentication codes of related cluster head.

Table: A typical table being maintained for the cluster head informations of their ID, PRNs their authentication code.

Cluster Head ID	Pseudo Random No.	Authentication Code
58565452	5	5a747675
	9	0d03010e
	…	..
69656362	13	0f030517
	16	4b474157

a) How to generate pseudo random number

Here we use well known method known as Linear Congruential Generators to generate [7] pseudo random numbers by following iterative equation

$PRN_{n+1} = (aPRN_n + i) \bmod m$

Where the various integers used in above equation are:-

m is the modulus (m>0)

a is the multiplier (0< a<m)

i is the increment (0≤ i<m)

PRN0 is the starting value or seed (0≤ PRN0 <m)

PRNn+1 is the next pseudo random number after PRNn.

In our technique, we use only integer numbers. For this, the value of m, a, i and PRN0 are always integers. So it generates only integer pseudo random numbers.

b) How to generate authentication code

For the generation of authentication code we use sensor node ID and its pseudo random number applying following steps:Find out PRNth prime number and its first primitive root.

Convert 8-digit Cluster Head ID (CHID) into 32-bit binary (4 bit for each digit)

Convert PRN into 32-bit binary by padding 0's if necessary(4 bit for each digit)

Apply XOR operation between 32-bit CHID (result of step 1) and 32-bit PRN (result of step 2).

Apply Padding with the value of primitive root for 8-digit, convert it into 32-bit binary and again apply XOR with result of step-4.

The result of step 5 is then broken into 8 groups of 4-bits.

Convert 4-bit binary into equivalent decimal number.

The result is an authentication code.

c) How to encrypt/decrypt data

To encrypt data message, we apply symmetric key encryption technique and generate cipher text. Here with the help of pseudo random number we apply the encryption technique which uses following steps:

Find out PRNth prime number and its first primitive root

Convert data message into equivalent 4-bit binary of each digit.

Convert PRN into equivalent 4-bit binary for each digit

Equalize the length of both data and PRN by padding of 0's if necessary and perform XOR operation.

Convert 4-bit binary into equivalent decimal number.

Add the primitive root in resultant decimal number (point 4).

For the decryption reverse the above process.

d) Role of Base station to achieve security

Following steps are followed for authentication and data communication.

When any cluster head wants to communicate with the base station, the cluster head sends an authentication code to the base station. Now base station will search authentication code in its own database whether this authentication code is related to that cluster head ID or not. If authentication code does not match, then the base station assumes that the cluster head is not reliable/trusted. If authentication code matches for a particular cluster head ID, the base station gets corresponding PRN from database using which this base station can decrypt data message.

Cluster head transfers only authentication code. So if any attacker somehow gets that authentication code it cannot communicate the same. This is because, to complete communication process, it is necessary to know authentication code as well as pseudo random number but pseudo random number is not transferred between cluster head and base station. Therefore attacker is unable to encrypt the data message as required by the base station.

B. Result:

We developed a new methodology for key management system which is LEACH(key). It is modified through imposing over the existing LEACH protocol and then checked its impact on the sensor network life time.

Following graph shows the difference between LEACH, without any key management technique and our developed key management technique which is applied over LEACH, i.e. LEACH (key). The experiment/ simulation have been done 20 times and the average life time of the network is reduced by 5.08% i.e. our key management technique is very lightweight.

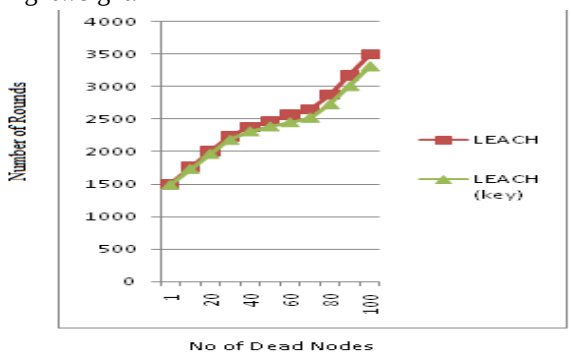

Figure 2.2: Comparison between LEACH and LEACH(key)

C. Malicious node detection

When we use hierarchal protocol (LEACH) for a wireless communication system, we use data aggregation technique which is discussed in above . In data aggregation technique, we create a trust based system where each node has a trust level. If the trust level of a node falls below the threshold level, we assume that this particular node is malicious node and is blocked i.e. that node is not allowed anymore to participate further in the communication. This way we find out the malicious node in networks also and discard it.

To identify the malicious node detection in a wireless sensor network we use following two techniques. First is Packet Monitoring System and second is Data Buffering Technique. Packet Monitoring System is useful in hierarchal protocols as well as in chain based protocols. Data Buffering Technique is useful in chain based protocol. Details of these techniques are as follows:

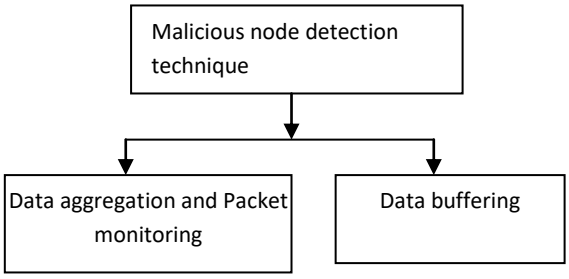

Figure 3.0:- Proposed techniques to detect the malicious nodes

- **The Packet Monitoring System:** This module checks the data sending rate of a node. We put two layers of threshold mechanism; lower threshold and upper threshold. If any node's sending rate is greater than that of a lower threshold but less than upper threshold, then that node may need observation to decide finally whether this node is malicious or not. For this we check its reliability by trust level of the node which is discussed in data aggregation technique in chapter 4. If the trust level is good, that means the node is not a malicious node. If the trust level is dubious- it is a malicious node and may be trying for flooding attack. If any node's sending rate is greater than that of upper threshold, then we directly declare that such a node is a malicious node.For example, let us take upper threshold value of data rate as 0.5 and lower threshold value as 0.4. Then if any node sends data more than 0.5 threshold then that node is malicious node. If sending rate is less than 0.4, then node is reliable for this module. If sending packet rate is between 0.4 and 0.5 then we check its reliability; if greater than one node is not malicious, otherwise node is malicious node.

Algorithm for packet monitoring system

Sending rate of the node is random value between 0-10.

Step1: Start packet monitoring system function.
Step2: Assign UT= 0.5 (upper threshold value)
Step3: Assign LT= 0.4 (lower threshold value)
Step4: sr= node(i).packet_to_ch *.5;
Step5: if sr>UT
Step6: node is malicious node
Step7: else
Step8: if node(i).priority<1
Step9: node is malicious node
Step10: otherwise node is reliable for communication.
Step11: endif(8) and endif(5)
Step12: end.

- **Data Buffering Technique:** This proposed mechanism is useful in chain based protocols. The message sender node observes the packet receiving node. It watches whether the receiver node alters the packet content or not. This is explained as below.

Once any node X sends data packet to node Y, node X acts as a monitoring node and observes the activities of node Y. When node Y sends data packet to next node, the node X listens and compares data with data sent by it to node Y. If the data is same, then node X ignores it. If it finds any difference between the data sent and data monitored, then node X demarcates node Y as a suspicious node. Every node creates a table of suspicious nodes that contains node ID and a number for suspicious and unsuspicious entries. It generates a threshold value. To start with the initial value of threshold is set as 0. Over a typical period, if a particular node sends suspicious data, then threshold value is incremented by 1 and if the data is unsuspicious then threshold value is decremented by 0.5. Finally when threshold value becomes more than 3, then the system declares it as a malicious node.

$$\text{threshold} = \text{threshold} + \begin{cases} 1, & \text{If Suspicious data} \\ -0.5, & \text{If Unsuspicious data} \end{cases}$$

Algorithm for data buffering technique
Step1: start buffering function
Step2: temp= node.data, th=0;
Step3: received_data= node(i).data.
Step4: if temp!=received_data
Step5: store node(i).ID
Step6: th=th+1;
Step7: else th=th-0.5
Step8: endif
Step9: if th>3
Step10: node(i) is marked as a malicious node.
Step11: otherwise node(i) is not malicious node. Endif(9)
Step12: end

D. The Experimental Evaluation:

MATLAB has been used to simulate the detection techniques for the malicious nodes. In a typical scenario, we take 100 nodes and get them randomly deployed in 100x100 meters2 area. A node transmission range is set of 25m, with default reliability 1, default probability of election of cluster head for LEACH as 0.1. In this simulation, all other parameters are constant so the analysis is based on the value of threshold_rate using our proposed MLEACH routing protocol and the data buffering technique.

Following graphs (Fig 3.1 to Fig 3.5) were obtained for typical threshold_rates. They show how network life time changes with different threshold rates.

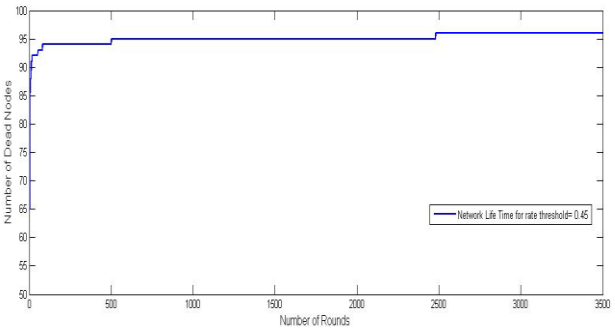

Figure 3.1:- Network life time in terms of no. of rounds when threshold_rate is 0.45

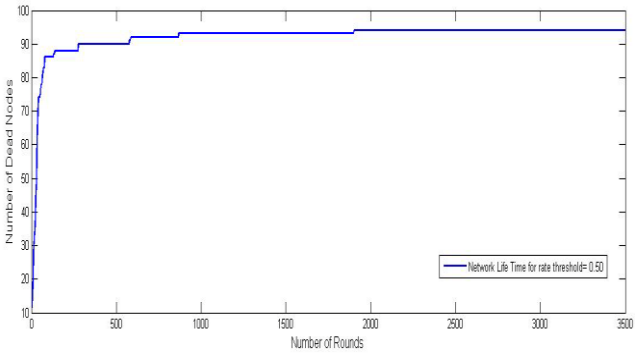

Figure 3.2:- Network life time in terms of no. of rounds when threshold_rate is 0.50

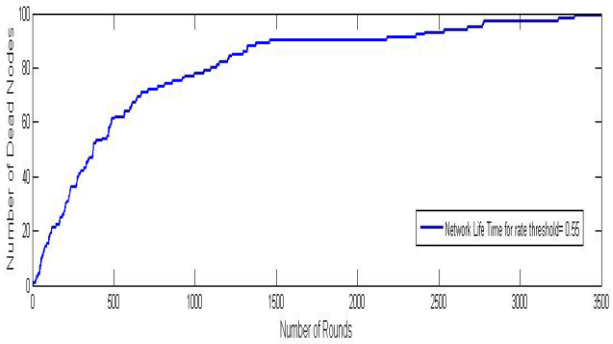

Figure 3.3:- Network life time in terms of no. of rounds when threshold_rate is 0.55

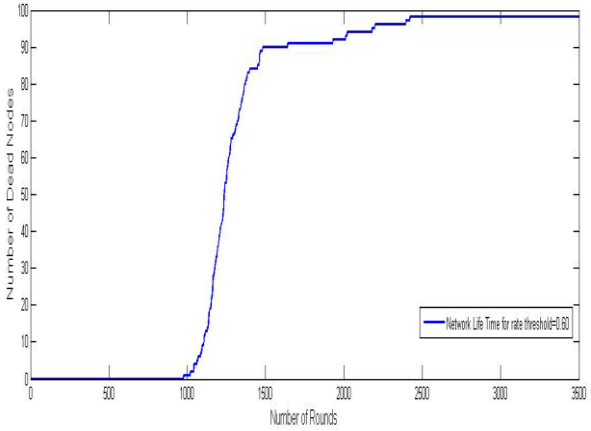

Figure 3.4:- Network life time in terms of no. of rounds when threshold_rate is 0.60.

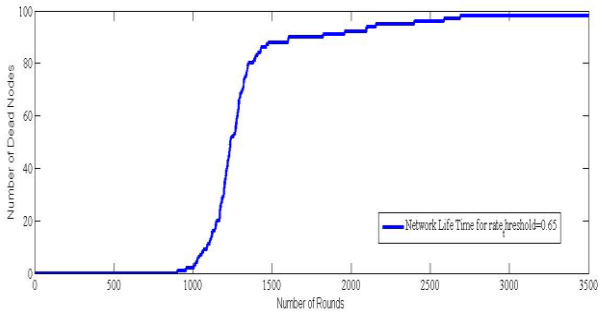

Figure 3.5:- Network life time in terms of no. of rounds when threshold_rate is 0.65.

Table 3.1:- Show the relation between threshold_rate and detected malicious nodes

Threshold_rate	Number of malicious Nodes
0.45	57
0.5	39
0.55	31
0.6	21
0.65	16

III. ANALYSIS OF THE PROPOSED SCHEME

Various results obtained in the above experiment are shown in fig. 3.1 to fig. 3.5. We observed that when we increase the threshold_rate, the number of malicious nodes declared to be dead decreases as shown in table below. At the same time it is also observed that if threshold value is too low then the number of suspected malicious node is high/more, which decreases the life span of a network. On the other hand if threshold value is too high then the number of suspected malicious node is minimum which decreases the reliability of a wireless sensor network. Therefore for efficient wireless sensor network, we require optimum threshold value which varies in limited range and may be decided on case to case basis.

IV. CONCLUSION

In this work we have proposed a novel security framework for WSN which has three layered architecture. First is the secure key management technique by which we create secure authentication along with encryption and decryption technique. Second is effective routing technique by which we reduce network overhead and improve life span of sensor nodes. In the present work we have modified two existing protocols LEACH and PIGASIS. Third is the malicious node detection technique by which we find out anomaly in the sensor network. Here we have used three techniques:- data aggregation, packet monitoring system using threshold mechanism and data buffering. This security framework is very light weight and all layers are independent from each other. So it can be easily installed in all type of wireless sensor network applications.

REFERENCES

1. John Paul Walter, Zhengqiang Liang, Weisong Shi and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey," Security in Distributed, Grid and Pervasive Computing, pp.1-50, 2006.
2. Abhishek Pandey and R.C. Tripathi, "A survey on Wireless Sensor Networks Security," International journal of Computer Applications, vol.3 no. 2, June 2010.
3. Eiji Nii, Takamasa Kitanouma, Naotoshi Adachi and Yasuhisa Takizawa, "Cooperative Detection for Falsification and Isolation of Malicious Nodes for Wireless Sensor Networks in Open Environment," 2017 IEEE Asia Pacific Microwave Conference(APMC), Nov 2017, pp.301-306.
4. Nikhil Kumar Mittal "A Survey on Wireless Sensor Network for Community Intrusion Detection Systems," 3rd International Conference on Recent Advances in information Technology(RAIT) 20016
5. AbduvaliyevAbror, Sungyoung Lee and Young-Koo Lee, "Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks," International Conference on Electronics and Information Engineering (ICEIE 2010), Kyoto, pp. v2-25- v2-29, 1-3 Aug. 2010.
6. Mohamed Ben Haj Frej, Khaled Elleithy, "Secure Data Aggregation Model (SDAM) in Wireless Sensor Networks," 14th International Conference on Machine Learning and Applications, pp. 330-334, 2015.
7. William Stallings,"Cryptography and Network Security," Fourth Edition, 2006.
8. Xi Luo Yi-Ying Zhang, Wen-Cheng Yang, Myong-Soon Park, "Prevention of DoS Attacks Based on Light Weight Dynamic Key Mechanism in Hierarchical Wireless Sensor Networks," Second International Conference on Future Generation Communication and Networking, Sanya, Hainan Island, Chaina, pp. 309-312, 2008.
9. AykutKarakaya, SedatAkleylek, "A Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks, 6th International Symposium on Digital Forensic and Security, Antalya, Turkey, pp. 581-585, March 2018.

AUTHORS PROFILE

Dr. Abhishek Pandey is working as Assistant Professor at IIIT-Lucknow, he has completed his M.Tech and PhD from IIIT-Allahabad, his research area includes , Wireless Security, Wireless Networks etc.

Dr. Lokendra Kumar Tiwari is working as Assistant Professor at Ewing Christian College, University of Allahabad, he has completed his MS from IIIT-Allahabad and PhD from University of Allahabad his research area includes, Information Security, Cyber Crime, Digital Forensics etc.